

MAR 21 2007

Attorney Docket No. 40116/03701 (1546)

REMARKS**I. INTRODUCTION**

Claims 1, 13 and 24 have been amended. Support in the specification for the above amendments may be found in at least page 10 and Fig. 3 of the Specification. No new matter has been added. Claims 1-29 remain pending in the above application. In view of the above amendments and following remarks, it is respectfully submitted that all pending claims are allowable.

II. THE 35 U.S.C. § 103(a) REJECTIONS SHOULD BE WITHDRAWN

The Examiner has rejected claims 1-29 under 35 U.S.C. § 103(a) as obvious over the U.S. Patent No. 5,790,536 to Mahany et al. ("Mahany") in view of U.S. Patent Application Publication No. 20040172536 to Malville et al. (hereinafter "Malville").

Mahany discloses a communication network containing a two-dimensional code reading device configured with a transceiver to send signals representative of captured two-dimensional images to one of the plurality of processors for decoding. (See, Mahany, col. 4, ll. 51 - 61). Images received within the processing circuit are compared to images within a database, and upon successful image decoding, the processor sends signals back to the code reading device representing the identified database comparisons for the images. (See, Id., col. 4, ln. 62 - col. 5, ln. 12). Authenticated images may be stored at the processing terminal and later compared to recorded images in order to establish communication between the two network devices. (See, Id., col. 71, ll. 18 - 20). The invention of Mahany only establishes communications between devices based on the type of data recorded at the reading device (e.g., keyed inputs, voice data, recorded images, etc.) and the routing information corresponding to the recorded data. (See, Id., col. 70, ll. 24-31, ll. 42-60).

Malville describes mutual PIN authentication of a mobile 10 and an access terminal 20 requiring an additional authentication server 30. (See, Malville, p. 5, ¶¶ [0099], [0104], Fig. 2c). According to Malville, the PIN authentication between mobile 10 and

Attorney Docket No. 40116/03701 (1546)

terminal 20 requires the mobile to send the terminal 20 its unique identifier MSISDN, the PIN, and a random number. (See, Id., p. 5, ¶ [0102]). Terminal 20 receives the PIN from mobile 10, but can not authenticate the user of mobile 10 until comparing the PIN entered to the PIN stored on server 30. (See, Id., p. 5, ¶¶ [0104]-[0105]). Malville differentiates biometric authentication of mobile 10 by terminal 20 from PIN authentication via mobile 10. (See, Id., p. 5, ¶ [0090]). Even though the biometric authentication of mobile 10 and terminal 20 does not involve server 30, the only way terminal 20 can authenticate the mobile 10 is by verifying the signature on the mobile 10's identifier MSISDN signed by an authority recognized by the terminal. (See, Id., p. 5, ¶¶ [0096] - [0097], Fig. 2b).

In contrast, claim 1 recites “sending an initial signal by the first device to establish a wireless communication with the second device, the first device including only a data capturing arrangement (“DCA”) as an input device interface with a user thereof”, “initiating an authentication process by the second device”, “obtaining a PIN code from the user via the DCA, the PIN code being obtained by the DCA from indicia on the second device”, “performing a pairing process to compare the PIN code to entries in a database of authorized PIN codes” and “when the pairing process has been successfully completed, generating a link key to establish the authenticated wireless communication between the first and second devices.”

Applicants respectfully submit that Mahany does not teach “obtaining a PIN code from the user via the DCA, the PIN code being obtained from indicia on the second device” or “generating a link key to establish the authenticated wireless communication between the first and second devices.” Specifically, Mahany merely describes comparing recorded two-dimensional images to stored images in an image database. However, the images recorded by code reader 4901, 4917 or 4929 are not obtained from indicia on host computer 4915, 4927 or 4947 or on any other device with which code reads 4901, 4917, or 4929 is to communicate. Rather, code reader 4901, 4917 or 4929 must read 2-D code 4903, 4919 or 4945 from container 4905 or 4921. (See Mahany, Figs. 49a-c). Moreover, Mahany

Attorney Docket No. 40116/03701 (1546)

neither teaches or describes a link key establishing the authenticated communication between computer or terminal. Thus, Mahany fails to teach each and every limitation of claim 1.

The examiner cites Malville to cure the defects of Mahany. It is respectfully submitted that Malville also fails to teach or describe "obtaining a PIN code from the user via the DCA, the PIN code being obtained by the DCA from indicia on the second device" or "generating a link key to establish the authenticated wireless communication between the first and second devices." Unlike the claimed invention, Malville requires there be more than just a first and a second device to provide PIN authentication. Instead, the PIN authentication of Malville requires an authentication server 30 to provide the stored PIN for comparison with the user-entered PIN. However, neither the authentication server 30 or terminal 20 are described as having indicia from which a PIN may be obtained by only a data capturing arrangement. Instead, Malville requires the user to enter the PIN via input keys in order to achieve authenticated communication. Therefore, the invention of Malville not only lacks a PIN being obtained from indicia on the server 30 or terminal 20, but fails to describe the PIN being obtained by only a data capturing arrangement.

Applicants further submit that Malville does not teach "generating a link key to establish authenticated wireless communication between the first and second devices." The signed token certifying the identity of the mobile telephone is not a link key establishing authenticated wireless communication between the mobile 10 and the terminal 20. At the point of issuance of the signed token, the invention of Malville still requires a further necessary authentication between the terminal and the mobile gateway. Therefore, the signed token does not establish a truly authenticated wireless communication between all the devices described in Malville (i.e., the mobile 10, terminal 20, and server 30). Malville also describes the mutual authentication of a portable object and a public access terminal but fails to describe any link key generated as a result of this authentication which establishes authenticated wireless communications. Thus, Malville discloses mutual authentication techniques between devices but never teaches or describes that the communications which follow after these mutual authentications are authenticated wireless communications.

Attorney Docket No. 40116/03701 (1546)

Therefore, Malville fails to teach or describe “obtaining a PIN code from the user via the DCA, the PIN code being obtained by the DCA from indicia on the second device” or “generating a link key to establish the authenticated wireless communication between the first and second devices” and fails to cure the defects of Mahany with respect to claim 1.

Applicants respectfully submit that Mahany or Malville, either alone or in combination, fail to teach or describe “obtaining a PIN code from the user via the DCA, the PIN code being obtained by the DCA from indicia on the second device” and “when the pairing process has been successfully completed, generating a link key to establish the authenticated wireless communication between the first and second devices,” as recited in claim 1. Therefore, the rejection to claim 1 under 35 U.S.C. § 103(a) must be withdrawn and claim 1 must be allowed. Because claims 2-12 depend on, and therefore include all the limitations of, claim 1, these claims are also allowable.

Claim 13 recites “a first wireless mobile device including only a data capturing arrangement (“DCA”) as an input device interface with a user thereof”, “a second device receiving an initial signal from the first device to establish a wireless communication, the second device initiating an authentication process, wherein the first device obtains a PIN code from the user via the DCA, the PIN code being obtained by the DCA from indicia on the second device, wherein the first and second devices perform a pairing process to compare the PIN code to entries in a database of authorized PIN codes, and wherein, when the pairing process has been successfully completed, the first and second devices generate a link key to establish the authenticated wireless communication.”

Claim 13 contains substantially the same limitations as recited in claim 1. Therefore, claim 13 should be made allowable for at least the same reasons cited above with respect to claim 1. Because claims 14-23 depend on, and therefore include all the limitations of, claim 13, these claims are also allowable.

Attorney Docket No. 40116/03701 (1546)

Claim 24 recites “a processor”, “a wireless communication arrangement” and “a data capturing arrangement (“DCA”) being the only input device interface for a user thereof, wherein the processor generates a request for establishing an authenticated wireless communication, the request being forwarded to the further device via the communication arrangement, the communication arrangement receives from the further device first data and a request for second data, the DCA obtaining the PIN code from the user, the PIN code being obtained by the DCA from indicia on the further device....”

Claim 24 also contains substantially the same limitations as recited in claims 1 and 13. Therefore, claim 24 should be made allowable for at least the same reasons cited above with respect to claims 1 and 13. Because claims 25-29 depend on, and therefore include all the limitations of, claim 24, these claims are also allowable.

RECEIVED
CENTRAL FAX CENTER

MAR 21 2007

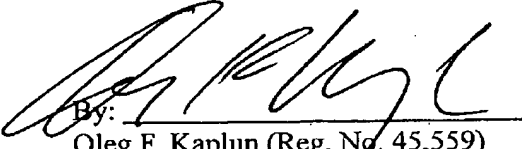
Attorney Docket No. 40116/03701 (1546)

CONCLUSION

In view of the above remarks, it is respectfully submitted that all the presently pending claims are in condition for allowance. All issues raised by the Examiner having been addressed, an early and favorable action on the merits is earnestly solicited.

Respectfully submitted,

Dated: March 21, 2007


By: _____
Oleg F. Kaplun (Reg. No. 45,559)

Fay Kaplun & Marcin, LLP
150 Broadway, Suite 702
New York, N.Y. 10038
(212) 619-6000 (telephone)
(212) 619-0276 (facsimile)